

---

# Cyberskepticism: The Mind's Firewall

By Timothy L. Thomas

**Editorial Abstract:** *Mr. Thomas examines various forms of computer network-related deception, including technical and social exploitation. He examines how deceptive practices can be easily concealed within existing cultural and network constructs. Finally, he advises adoption of a proper mental framework to help defeat this class of cyber threats.*

## Introduction

In 2004, computer hackers in the Netherlands developed a way for unsuspecting computer users to download a virus. Their vessel for doing so was a photo of Russian tennis star Anna Kournikova, a heart throb to many young male tennis enthusiasts. As *SearchWindowsSecurity* reported:

*The Anna Kournikova VBS.SST computer virus, informally known as "Anna," is a viral worm that uses Visual Basic to infect Windows systems when a user unwittingly opens an e-mail note with an attachment that appears to be a graphic image of Russian tennis star Anna Kournikova. However, when the file is opened, a clandestine code extension enables the worm to copy itself to the Windows directory and then send the file as an attachment to all addresses listed in your Microsoft Outlook e-mail address book.*

Such cyber deception is, unfortunately, quite common. Episodes involving cyber deception occur daily and, in some of the worst cases, have resulted in suicides, identity theft, financial scandals, assists to pedophiles, and "cybercide" (inadvertently taking down your own network by downloading and propagating a virus). Most recently hackers have tried to penetrate the Pennsylvania Lottery. Consider the ramifications and consequences if they are successful in this endeavor!

The context that ignites cyber deception is the similarity between reality and digitally generated forms of communication (text, video, etc.). This confrontation was fully brought into focus in the 1983 film *War Games*. A computer named Joshua, while playing a game initiated by young computer wizard David Lightman (actor Matthew Broderick), takes control of all US nuclear weapons and begins a count down to launch them and start World War III. Lightman asks Joshua if he is playing the game or playing for real. Joshua answers: "What's the difference?"

Cyber deception utilizes the similarity between reality and digital communication to exploit cognitive biases in human decision-making. These biases prey on a human's proclivity to accept rewards, romance, charity, or other feelings of sensitivity and emotion; or in some cases exploit habits or environmental influences (gambling, participation in scams, etc.). Since real issues and digital issues often coincide, humans are easily enticed into believing that what is false is real, and vice versa.

This article explains the context within which cyber deception has fermented. It then offers several examples of the forms that cyber deception has taken in recent years. The study of cyber deception has obvious value for a military audience—it is a key element of IO and OPSEC. In fact, some of the best OPSEC advice available is to "be a cyberskeptic."

## Social Engineering

Information security expert Mark Edmead, writing about famed computer hacker Kevin Mitnick (who exploited human vulnerabilities to the maximum extent possible), noted:

*According to Mitnick, all of the firewalls and encryption in the world will never stop a gifted social engineer from rifling a corporate database or an irate employee from crashing a system. If an attacker wants to break into a system, the most effective approach is to try to exploit the weakest link—not operating systems, firewalls or encryption algorithms—but people.*

Pitting one's cognitive skills and beliefs against a person or system to access a product, a password, or some other type of information is a process known as social engineering. *Wikipedia* defines social engineering as:

*"A collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim."*

Social engineering tries to fool decision makers, and is really nothing more than an updated term for stratagems used by the Chinese thousands of years ago for similar purposes. There are many social engineering techniques, several of which are highlighted below:

- **Pretexting**—the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is typically done over the telephone.
- **Phishing**—a technique of fraudulently obtaining private information, typically by sending an e-mail that looks legitimate.
- **IVR/phone phishing**—technique using an Interactive Voice Response (IVR) system to recreate a legitimate sounding copy of a bank or other institution's IVR system.
- **Trojan horse/gimmies**—technique taking advantage of a victims' curiosity or greed to deliver malware.
- **Road apple**—a real-world variation of a Trojan Horse using physical media and relying on a victim's curiosity



Kevin Mitnick, Noted Social Engineer.  
(Matthew Griffiths, *Wikipedia.org*)

(leaving a CD or USB flash drive in a place where it will be found).

- *Quid pro quo*—technique involving a random caller who states that he is from technical support in an attempt to find someone with a problem and then guide them through commands giving the caller access or the ability to launch malware.

Cyber deception exploits in electronic fashion older deception techniques known as “confidence tricks.” These are the con games or scams that try to swindle a person after gaining their confidence. Confidence tricks enable cyber deception successes in get-rich-quick schemes; romance, extortion, gambling, false injury or false reward, and charity tricks; and undercover cop scams, among others.

### A Fertile Playing Field

The number of cybersites that consumers depend upon daily has grown considerably over the past several years. A tiny fraction of the digital playing field includes: e-mail; *MapQuest*; *Google*; *FaceBook*; *Flickr*; *MySpace*; *phonebook*; *BitTorrent*; *iTunes*; *YouTube*; forums; chat rooms; dating; *Craig’s List*; donate; blog/vlog; video games; e-invitations; e-cards; weather; text messaging; financial planning; personal websites; picture sharing; airline travel; banking; test preparation; college classes; and cell phones.

Within these cyber circles, especially when *FaceBook* and *MySpace* were startups, common ideological thought or interests served as strong bonds. Virtual trust accumulates among individuals or groups even though an actual “meeting” has never occurred. Cyber tribes form. Unfortunately, as virtual trust grows so does virtual and cognitive vulnerability. For example, someone posing as an adherent to a cause can enter a group and gather information, manipulate the group’s way of thinking, or embarrass the group by pretending to be a group member but publicly criticizing its cause. This can fool readers of a website into believing that group members are not cohesive, among other consequences.

Virtual size is another factor influencing cognitive deception. On the Web, it is very easy for one or a few people to appear to represent thousands simply through the number of messages produced. Virtual quantity, as the saying goes, has a virtual quality (in this case sheer size and thus influence) all its own that persuades via peer pressure or some other uniting factor.

While the main focus of cyber deception is to manipulate a person’s cognitive perceptions, software can be manipulated as well (since humans write it!). Software is the unsuspecting

agent that spreads false, selective, or viral material. Web crawlers are one of the most obvious tools that can produce cyber deceptive material. For example, they can determine website content. Depending on how an algorithm is written, a Web site will gather some data and discard others. An Al Qaeda website may eliminate all information about Christianity, thus deceiving subscribers about both the nature and popularity of the religion. In this case it can be both false and selective.

In another instance, Web crawlers are often designed to match advertising to fit the content of the website. Some of those advertisements could be illusions of grandeur designed only to collect money from unsuspecting readers. Machines and software thus begin to control people through monitoring and manipulation. The cyber deception malady is present in both people and software.

While criminals and terrorists use cyber deception to collect data, cyber deception can also be used by website moderators to provide false information to the consumers visiting the

site. In fact, cyber deception is one of the most common ways for law enforcement personnel to catch pedophiles.

Nicholas Carr, former executive editor of the *Harvard Business Review*, believes that artificial intelligence experts have not only succeeded in rewiring our computers but humans as well. From his point of view, people are beginning to process information as if they were nodes with regard to speed of locating and reading data. If we only tend to go to certain websites, then much like Web crawlers we only access certain types of information. This allows machines to transfer their way of thinking into humans—if the latter

don’t take the time to process and analyze the information.

Of course, there are a plethora of cyber deception examples from which to choose. Even a small selection demonstrates the widespread use of cyber deception. They also demonstrate any source, no matter how trustworthy, can turn into a cyber deceiver, sometimes without the source’s knowledge.

### Cyber Deception From an Unlikely and Trusted Source

One example of cyber deception from a trusted source involved the *San Francisco Chronicle*. The paper’s website, *SFGate.com*, posted comments from readers. The paper’s moderators found a way to ‘neuter’ what they considered problem comments. The moderators were able to do so without making it appear that a comment had been eliminated due to ideological concerns. Their methodology went as follows. When a problem comment appeared, the moderators found a cyber or digital way to eliminate the comment from the Web



(US Navy)

***“... any source, no matter how trustworthy, can turn into a cyber deceiver.”***

page for all viewers *except* from the person who submitted it. That way, the person submitting the comment was satisfied that his or her opinion had been expressed and was still “out there” on the Web. The moderator’s deception was exposed when a person who had submitted a “problem” comment tried to view his comment from a computer other than his own (he wanted to show it to a friend). His comment was not there. He returned home and found the comment still on his personal computer. He then wrote to the *Chronicle* and they admitted the cyber deception. This group carried out dual cyber deception: the moderators fooled both their public into thinking there wasn’t any criticism of the type leveled by the individual, and the individual was cyber deceived into thinking his posting was still online.

Another case of cyber deception was based on comments from entrepreneur Dan Ackerman Greenberg. He described some secret strategies behind the creation of viral videos—those Internet videos that really take off and become popular “must sees” such as Soulja Boy, Miss Teen South Carolina, and Smirnoff’s Tea Partay music video. In essence, his strategies to make videos viral were cyber deception methods. For instance, he recommended paying people who run relevant blogs to post embedded videos. As a result, what “seems” popular has actually been pre-financed through blog masters, thus cyber deceiving the audience (“this video is on the most watched list, it must be good”). Greenburg would also create huge friend lists on *Facebook* and then send all of them a video. He would ask that his friends e-mail the video to their friends, or at least share it on *Facebook*. He would also change the name of the video so that it would appear new, though people were simply visiting the same site. At times he would have conversations with himself, recommending the video to others, or have others in his office post comments about the video and get a heated conversation going about the video. Thus his virtual conversations and other methods acted to cyber deceive many people, causing them to either watch the video or go find it, because it appeared popular. Greenberg concludes by noting that “true virality takes serious creativity.” Virtual creativity is thus another cyber deception methodology for IO professionals to explore.

### **Cyber Linking the Virtual World With the Real World (Especially Romance)**

In January of 2007, storms were battering Europe and more than 230 people had died. On the Web there appeared an article called “Full Story.exe.” While providing more information on the storm, the story provided a damaging storm of another type. The file, of course, contained a virus dubbed the “Storm Worm.” As *Time* magazine reported:

*... the virus is a marvel of social engineering and “it is to viruses what Michelangelo was to ceilings.” Its subject line changes constantly, it preys on shock, outrage, prurience, and romance. It mutates quickly, changing its size and tactics often to avoid virus filters. It exploits blogs and bulletin boards. It contains links to fake YouTube pages which crash your browser.*

*More importantly it provides others with access and control over your computer.*

Real-world romance techniques on the Internet have produced some very innovative cyber deception techniques. Valentine cards sent electronically are one technique designed to enhance romance. In 2006 electronic Valentine cards were sent to unsuspecting people who opened them for various reasons (do I have a secret lover?). Some of the messages arrived “having been forwarded by or appearing to have been forwarded by people known by the recipient.” While piquing one’s curiosity, it also tricked people into infecting their computers.

Recently, the Russian language website CyberLover.ru was identified as capable of holding “fully automated flirtatious conversations with users of chat-rooms and dating sites, to persuade them to share their identity or visit websites with malicious content.” An English version of the site has not yet appeared. The site can establish a relationship with up to ten people in thirty minutes, and purportedly its victims cannot tell whether there is a human or a computer generated response on the other end. Sergei Shevchenko, a *PC Tools* senior malware analyst, says the site “monitors the victims’ Internet browser activity, automatically recognizes and fills in fields in the Web pages, generates keystrokes and mouse clicks, and posts messages, URLs, files, and photos.” Clearly this is a marvel of current cyber social engineering and deception skills.

### **Cyber Deceptive Visitors**

Important websites, such as those run by NASA, the US Army, hospitals, or the UK’s Ministry of Defense, are visited thousands of times each month by people from all over the globe. Not all visits are innocuous, however. Several visitors are most likely intended or designed to simply gather data. Some may also use anonymizers to hide their true identities. The UK’s Counter Terrorism Science and Technology website recently posted “who” had visited its website, to include potential suppliers. Information of this sort can be “precisely the kind of fodder gathered in foot printing exercises, in which attackers learn as much as possible about sites they intend to penetrate.”

### **Cyber Deceptive RFID Tags**

A radio-frequency identification (RFID) tag is a chip with imbedded data. When the tag “hears” a particular radio signal, it broadcasts its number, thus becoming “located.” Such chips are implanted in dogs, books, and other articles to find them when they are lost. However, if the tag is removed and placed in another receptacle, then those seeking the chip will be cyber deceived into running after another source. You may be searching for a German Shepherd, but may instead locate a horse, sheep or snake depending on who hosts the chip. A more sophisticated use of the RFID chip would be stealing information from passports or security cards, which also send out a signal. Someone walking near you with a reader could get your passport or security card information. Such information

could be placed in another chip or just the information itself could be used to confirm someone's identity. Some people have begun wrapping their passports in metal foil to make their information harder for RFID readers to access.

### **Cyber Deception to Breach Firewalls**

The November 2007 issue of *Wired* magazine provided a list of methods to breach information security. First, it was recommended to go 'in disguise.' Using this cyber deception method involves using proxy servers and other software to mask location and identity. Not long ago *Foreign Policy* magazine noted that a system known as Tor was "a downloadable software that routes an Internet surfing session through three proxy servers randomly chosen from a network of more than 1,000 servers run by volunteers worldwide." This cyber deception method frustrates law enforcement agencies from finding the source of a criminal or insurgent message. Keystroke tracking software installed on keyboards allows for cyber monitoring in cybercafés to keep track of messages being sent out without the user's knowledge. Of course cyber proxies could be used against any target. Other more straightforward methods suggest common sense ideas, not nearly as sophisticated. These include scrambling messages using encryption, posting on sites rarely monitored, searching overseas versions of a website, avoiding controversial terms, and using Skype [internet protocol telephone].

### **Cyber Deceptive Advertising**

Some eighteen months ago, *MySpace* ran online banner ads infected with adware. This allowed malware to surreptitiously track infected users' Internet usage while bombarding them with pop-up ads. In a similar episode, users were invited to download a Sudoku game to pass the time. Attached to the Sudoku game advertisement was adware providing the same type of cyber tracking.

### **Cyber Deception Techniques Of a Hacker**

Noted social engineer Kevin Mitnick, who was arrested and served time in prison for hacking into computers, wrote the best book on cyber deception available on the market today. Titled *The Art of Deception*, he describes how he enticed people into providing passwords and codes through social engineering techniques.

Mitnick noted that firewalls and biodetection systems are great ways to prevent hacking, but that training people to spot social engineering techniques is just as important. For example, one way to get information on cyber access codes is to call an unsuspecting person at a company and pose as an associate. This initial discussion will focus on troubleshooting a nonexistent network problem for the unsuspecting person. After pretending to have fixed the problem, Mitnick says the "associate" would ask for a favor, playing on a human tendency to reciprocate for a good deed. He notes this "causes people to take a mental shortcut, based not on the request, but the favor."



*Practicing cyberskepticism. (US Army)*

### **Cyber Phishing**

No discussion of cyber deception would be complete without a discussion of phishing techniques. According to *Wikipedia*, phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing often directs users to enter details at a website. Current attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical measures.

Among the thousands of phishing scenarios, several come to mind. One was the attempt to access personnel databases on people who had visited the Oak Ridge National Laboratory, starting from 1990. Staff members received hoax emails that at first glance appeared legitimate. Such messages gave information to members of a scientific conference and another pretended to have information about a Federal Trade Commission complaint.

### **Cyber Deception and Hoaxbusters**

In an odd way, explicit warnings about viruses, and our concern about downloading a virus inadvertently, have helped spawn a number of Internet virus hoaxes. A hoax uses a hook, a threat, or a request to get someone to believe in a fake message or chain letter and send it on to someone else or take some sort of action. Hoaxes adopt many of the principles associated with social engineering. The website <http://hoaxbusters.ciac.org> has listed a series of hoax categories: malicious code warnings; giveaways; chain letters; urban myths; sympathy hoaxes; threats; inconsequential warnings; scams; scare chain letter; jokes; true legends; hacked history; and stories with unknown origins.

### **Cyber Deception By Insurgents**

Insurgents now plan, recruit, teach, and finance on the Internet. Further, they deceive through a variety of techniques that military planners must consider. A member of the US Army Foreign Military Studies Office (FMSO) accidentally discovered one of the most interesting techniques. It involved a cyber deception strategy known as "hide in plain site."

The FMSO analyst was looking over a website focused on Arab entertainment. By chance, his hand slipped on the mouse and pulled the cursor to the bottom of page two. There, out of site unless you knew it was there, was a counter mechanism counting backwards to zero. Then the counter disappeared. Curious, the analyst got out of the site and went back in, immediately scrolling to the bottom of page two. Again he saw the counter before it disappeared. Once again, the analyst exited the website and reentered, but this time he clicked on the counter. The link took him directly to an extremist insurgent website. This is cyber deception of a still different type, in which the access point ‘cybervanished’ after a certain time period.

### **Cyber Address Book Harvesting**

Some programs are specially designed to steal the computer address book of, let’s say, Mister X. When this occurs, the address “harvester” then uses the address book to send out spam or viruses with the added line “this email was sent to you on behalf of person X,”—the one whose address book was stolen. Since the information was sent to you on behalf of someone you already know and regularly correspond (X), more often than not the intended target will open the email.

### **Cyber Deception Via Satellite**

The Russian military has explored the use of cyber deception’s adaptation to a concept known as ‘reflexive control’ (similar, but not identical, to the US term ‘perception management’). Reflexive control (RC) consists of transmitting motives and grounds from the controlling entity to the controlled system that stimulate a desired decision. The goal of RC is to prompt the enemy to make a decision unfavorable to him. Naturally, one must already have a good idea about how the enemy thinks to make such attempts successful.

Russian theorist Colonel Sergei Leonenko initially thought the use of computers would hinder the use of reflexive control since computers would make it easier to process data and calculate options. A computer-aided opponent could more easily “see through” a reflexive control measure by an opposing force, due to greater speed and accuracy in processing information. He later surmised, however, that computer use may actually improve the chances for successful reflexive control, since a computer lacks a human being’s intuitive reasoning. Leonenko suggests acting against technical reconnaissance assets, especially weapons guidance systems, which are impassive in assessing what is occurring and do not perceive to what a person reacts. He believes we live in a frightening time if, in fact, decisions are in the hands of machines “incapable of assessing what is occurring, and do not perceive what a person reacts to.”


### **Conclusions**

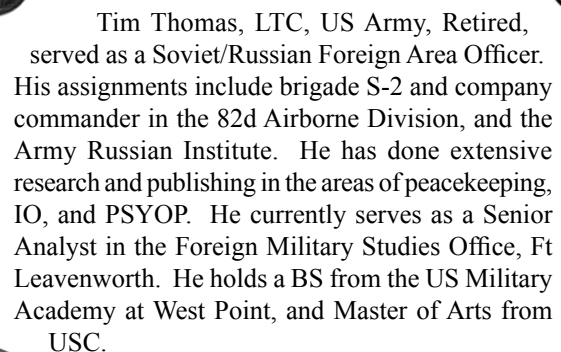
The major conclusion one can draw from this explanation is that in the cyber age, people have to develop

a strong sense of cyber skepticism. Skepticism should not be limited to computer operators; a healthy dose should be present in Blackberry, iPhone, cell phone, and other digital device users. Without skepticism, users and operators are almost certainly doomed to exploitation by electrons somewhere, sometime. The article you are now reading could also have elements of cyber deception, since much of the information was taken from the Internet without a sure way of confirming the material’s authenticity!

Cyber deception has practically evolved into an art form. It is creative, invasive, and, as Kevin Mitnick noted, strongly dependent on social engineering techniques. Before the development of the personal computer, people were fooled by confidence tricks. But these same people were never exposed to the onslaught of cyber deception attempts, nor the consequences of successful attempts (the emptying of your bank account is but one possible result) that people experience today.

The number of terms involved with cyber deception causes confusion among computer users who are not dedicated to the study of information security issues. This also increases a computer user’s susceptibility to attack. For example, a recent BBC report listed several cyber deception techniques other than those listed above. The average home computer user may not totally understand the effects of the following: pharming (fraudsters redirect net users from legitimate to fake sites); rogue dialing (software that installs itself on computers and changes settings to dial a premium rate number instead of usual dialup accounts); spyware (small programs that secretly monitor sites visited); keylogging (software/hardware to track keystrokes on a computer to gather passwords and credit card numbers); and other terms related to deceptive scams on personal computers.

The bottom line: be a cyberskeptic. Only in this way can we erect an effective cognitive defense against the many forms of cyber deception. The mind has no firewall—except skepticism. 



Tim Thomas, LTC, US Army, Retired, served as a Soviet/Russian Foreign Area Officer. His assignments include brigade S-2 and company commander in the 82d Airborne Division, and the Army Russian Institute. He has done extensive research and publishing in the areas of peacekeeping, IO, and PSYOP. He currently serves as a Senior Analyst in the Foreign Military Studies Office, Ft Leavenworth. He holds a BS from the US Military Academy at West Point, and Master of Arts from USC.